

Refine Search

Search Results -

Terms	Documents
L19 and L17	2

Database:

US Pre-Grant Publication Full-Text Database
 US Patents Full-Text Database
 US OCR Full-Text Database
 EPO Abstracts Database
 JPO Abstracts Database
 Derwent World Patents Index
 IBM Technical Disclosure Bulletins

Search:

L20

Refine Search

Recall Text

Clear

Interrupt

Search History

 DATE: Thursday, April 28, 2005 [Printable Copy](#) [Create Case](#)

<u>Set</u> <u>Name</u> side by side	<u>Query</u>	<u>Hit</u> <u>Count</u>	<u>Set</u> <u>Name</u> result set
<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR</i>			
<u>L20</u>	L19 and l17	2	<u>L20</u>
<u>L19</u>	L18 and @ad<=19980414	2	<u>L19</u>
<u>L18</u>	L16 and (tag\$ or label\$)	19	<u>L18</u>
<u>L17</u>	L16 and @ad<=19980414	2	<u>L17</u>
<u>L16</u>	L15 and tag\$	19	<u>L16</u>
<u>L15</u>	L13 and (crypto\$ or encrypt\$ or decrypt\$)	77	<u>L15</u>
<u>L14</u>	L13 and (electronic\$ near2 tag\$)	0	<u>L14</u>
<u>L13</u>	"zero knowledge protocol" and authenticat\$	80	<u>L13</u>
<i>DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR</i>			
<u>L12</u>	L11 and zero\$	2	<u>L12</u>
<u>L11</u>	5546463.pn. or 5303370.pn. or 6363483.pn. or 6069955.pn. or 5878142.pn. or 5666417.pn. or 5640002.pn. or 5574790.pn.	8	<u>L11</u>

*DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES;
OP=OR*

<u>L10</u>	L9 and modular\$	15	<u>L10</u>
<u>L9</u>	L8 and ((self\$ or automatic\$) with dispens\$)	60	<u>L9</u>
<u>L8</u>	(parabol\$ with (shape or form\$)) and @ad<=20011222	14073	<u>L8</u>
<u>L7</u>	L6 and parabol\$	2	<u>L7</u>
<u>L6</u>	L5 and ((self\$ or automatic\$) with dispens\$)	60	<u>L6</u>
<u>L5</u>	L2 and @ad<=20011222	237	<u>L5</u>
<u>L4</u>	L3 and l2	3	<u>L4</u>
<u>L3</u>	221/9,13.ccls.	961	<u>L3</u>
<u>L2</u>	L1 and (work adj station) and hous\$	416	<u>L2</u>
<u>L1</u>	dispens\$ and display\$	67109	<u>L1</u>

END OF SEARCH HISTORY

Hit List

Clear	Generate Collection	Print	Fwd Refs	Bkwd Refs
Generate OACS				

Search Results - Record(s) 1 through 2 of 2 returned.

☐ 1. Document ID: US 6434238 B1

Using default format because multiple data bases are involved.

L17: Entry 1 of 2

File: USPT

Aug 13, 2002

US-PAT-NO: 6434238

DOCUMENT-IDENTIFIER: US 6434238 B1

**** See image for Certificate of Correction ****

TITLE: Multi-purpose transaction card system

DATE-ISSUED: August 13, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chaum; David	Sherman Oaks	CA		
Ferguson; Niels	Amsterdam			NL
Van Der Hoek; Jelte	Amsterdam			NL

US-CL-CURRENT: 380/45; 380/30, 705/67, 713/172

Full	Title	Citation	Front	Review	Classification	Date	Reference			Claims	FIGS	Draw. Des
------	-------	----------	-------	--------	----------------	------	-----------	--	--	--------	------	-----------

☐ 2. Document ID: US 5297206 A

L17: Entry 2 of 2

File: USPT

Mar 22, 1994

US-PAT-NO: 5297206

DOCUMENT-IDENTIFIER: US 5297206 A

TITLE: Cryptographic method for communication and electronic signatures

Full	Title	Citation	Front	Review	Classification	Date	Reference			Claims	FIGS	Draw. Des
------	-------	----------	-------	--------	----------------	------	-----------	--	--	--------	------	-----------

Clear	Generate Collection	Print	Fwd Refs	Bkwd Refs	Generate OACS
-------	---------------------	-------	----------	-----------	---------------

Terms	Documents
L16 and @ad<=19980414	2

Display Format: **Change Format**

[Previous Page](#)

[Next Page](#)

[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)

Generate Collection

Print

L17: Entry 1 of 2

File: USPT

Aug 13, 2002

US-PAT-NO: 6434238

DOCUMENT-IDENTIFIER: US 6434238 B1

**** See image for Certificate of Correction ****

TITLE: Multi-purpose transaction card system

DATE-ISSUED: August 13, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chaum; David	Sherman Oaks	CA		
Ferguson; Niels	Amsterdam			NL
Van Der Hoek; Jelte	Amsterdam			NL

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
InfoSpace, Inc.	Bellevue	WA			02

APPL-NO: 08/ 909480 [PALM]

DATE FILED: August 11, 1997

PARENT-CASE:

This application is a continuation (under 35 USC.sctn.120/365) of PCT/US95/01765 designating the U.S. and filed Feb. 13, 1995 as, in turn, a continuation-in-part (under 35 .sctn. 120/365) of U.S. application Ser. No. 08/179,962 filed Jan. 11, 1994, now U.S. Pat. No. 5,434,919.

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 380/45; 705/67, 713/172, 380/30

US-CL-CURRENT: 380/45; 380/30, 705/67, 713/172

FIELD-OF-SEARCH: 380/30, 380/45-47, 235/380, 705/67-69, 713/169-172

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected

Search ALL

Clear

PAT-NO

ISSUE-DATE

PATENTEE-NAME

US-CL

3668653

June 1972

Fair et al.

4625276

November 1986

Benton et al.

<input type="checkbox"/>	<u>4630201</u>	December 1986	White	
<input type="checkbox"/>	<u>4742546</u>	May 1988	Nishimura	
<input type="checkbox"/>	<u>4747050</u>	May 1988	Bracht1 et al.	380/45
<input type="checkbox"/>	<u>4771376</u>	September 1988	Kamiya	
<input type="checkbox"/>	<u>4771461</u>	September 1988	Matyas	
<input type="checkbox"/>	<u>4877947</u>	October 1989	Mori	
<input type="checkbox"/>	<u>4881264</u>	November 1989	Merkle	
<input type="checkbox"/>	<u>4885777</u>	December 1989	Takaragi et al.	
<input type="checkbox"/>	<u>4906828</u>	March 1990	Halpern	
<input type="checkbox"/>	<u>4914698</u>	April 1990	Chaum	
<input type="checkbox"/>	<u>4935962</u>	June 1990	Austin	
<input type="checkbox"/>	<u>4947430</u>	August 1990	Chaum	
<input type="checkbox"/>	<u>4987593</u>	January 1991	Chaum	
<input type="checkbox"/>	<u>5005200</u>	April 1991	Fischer	
<input type="checkbox"/>	<u>5016009</u>	May 1991	Whiting et al.	
<input type="checkbox"/>	<u>5016274</u>	May 1991	Micali et al.	
<input type="checkbox"/>	<u>5034597</u>	July 1991	Atsumi et al.	
<input type="checkbox"/>	<u>5117458</u>	May 1992	Takaragi et al.	
<input type="checkbox"/>	<u>5131039</u>	July 1992	Chaum	
<input type="checkbox"/>	<u>5140634</u>	August 1992	Guillou et al.	
<input type="checkbox"/>	<u>5212788</u>	May 1993	Lomet el al.	
<input type="checkbox"/>	<u>5214702</u>	May 1993	Fischer	
<input type="checkbox"/>	<u>5220501</u>	June 1993	Lawlor et al.	
<input type="checkbox"/>	<u>5221838</u>	June 1993	Gutman et al.	
<input type="checkbox"/>	<u>5241599</u>	August 1993	Bellovin et al.	
<input type="checkbox"/>	<u>5247578</u>	September 1993	Pailles et al.	
<input type="checkbox"/>	<u>5267314</u>	November 1993	Stambler	
<input type="checkbox"/>	<u>5280527</u>	January 1994	Gullman et al.	
<input type="checkbox"/>	<u>5299263</u>	March 1994	Beller et al.	
<input type="checkbox"/>	<u>5311594</u>	May 1994	Penzias	
<input type="checkbox"/>	<u>5361267</u>	November 1994	Godiwala et al.	
<input type="checkbox"/>	<u>5373558</u>	December 1994	Chaum	
<input type="checkbox"/>	<u>5402490</u>	March 1995	Mihm, Jr.	
<input type="checkbox"/>	<u>5434919</u>	July 1995	Chaum	380/30
<input type="checkbox"/>	<u>5748737</u>	May 1998	Daggar	235/380

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 281 224	September 1988	EP	
0 291 834	November 1988	EP	
0 421 808	April 1991	EP	
0439847	August 1991	EP	
0 535 863	April 1993	EP	
0 573 245	December 1993	EP	
2 274 523	July 1994	GB	
WO 89/08957	September 1989	WO	
WO 90/04892	May 1990	WO	

OTHER PUBLICATIONS

Chaum et al, "Untraceable Electronic Cash", Advances in Cryptology--Crypto '88, pp. 319-327.

Even et al, "On-line/Off-line Digital Signatures", Advances in Cryptology--Crypto '89, pp. 263-275.

Box et al, SmartCash: A Practical Electronic Payment System, CWI Technical Report CS-R9035.

Diffie et al, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. IT22, No. 6, No. 79, pp. 644-654.

Lamport, "Construction Digital Signatures form a One Way Function", SRI Technical Report CSL-08.

"Matrix Digital Signature for Use With the Data Encryption Algorithm", IBM Technical Disclosure Bulletin, vol. 28, No. 2, Jul. 1985, pp. 603-604.

Merkle, "A Digital Signature Based on a Conventional Encryption Function", Advances in Cryptology--Crypto '87, pp. 369-378.

Chaum et al, "Undeniable Signatures", Advances in Cryptology--Crypto '89, pp. 212-216.

ART-UNIT: 2661

PRIMARY-EXAMINER: Cangialosi; Salvatore

ABSTRACT:

Disclosed is a multi-purpose transaction card system comprising an issuer, one or more cards, one or more terminals, and optionally one or more acquires, communicating using a variety of cryptographic confidentiality and authentication methods. Cards authenticate messages using public key based cryptographic without themselves performing the extensive computations usually associated with such cryptography. Integrity of complex transaction sequences and plural card storage updates are maintained, even under intentionally generated interruptions and/or modifications of data transmitted between card and terminal. Cards do not reveal any information to the terminal which is not directly necessary for the transaction or any information to which the terminal should not have access, though externally measurable aspects of its behavior. Transaction types supported include those suitable for off-line credit cards, in which the "open to buy" is maintained on the card.

10 Claims, 58 Drawing figures

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

[First Hit](#) [Fwd Refs](#)[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)**End of Result Set**

Generate Collection

Print

L17: Entry 2 of 2

File: USPT

Mar 22, 1994

US-PAT-NO: 5297206

DOCUMENT-IDENTIFIER: US 5297206 A

TITLE: Cryptographic method for communication and electronic signatures

DATE-ISSUED: March 22, 1994

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Orton; Glenn A.	Hamilton, Ont.			CA

APPL-NO: 07/ 957105 [PALM]

DATE FILED: October 7, 1992

PARENT-CASE:

CROSS REFERENCE TO RELATED APPLICATION This application is a continuation-in-part of my earlier filed U.S. patent application Ser. No. 07/854,389 filed Mar. 19, 1992 and now abandoned.

INT-CL: [05] H04L 9/30, H04L 9/32

US-CL-ISSUED: 380/30; 380/23, 380/28

US-CL-CURRENT: 380/30; 380/28, 713/174, 713/180

FIELD-OF-SEARCH: 380/30, 380/23-25, 380/28

PRIOR-ART-DISCLOSED:

U. S. PATENT DOCUMENTS

Search Selected

Search ALL

Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
<input type="checkbox"/>	<u>4306111</u>	December 1981	Lu et al.	380/30
<input type="checkbox"/>	<u>4399323</u>	August 1983	Henry	380/30
<input type="checkbox"/>	<u>4633036</u>	December 1986	Hellman et al.	380/30
<input type="checkbox"/>	<u>4748668</u>	May 1988	Shamir et al.	380/30 X
<input type="checkbox"/>	<u>4995082</u>	February 1991	Schnorr	380/30 X
<input type="checkbox"/>	<u>5016274</u>	May 1991	Micali et al.	380/30 X
<input type="checkbox"/>	<u>5054066</u>	October 1991	Rick et al.	380/30
	<u>5073935</u>	December 1991	Pastur	380/30

5097504

March 1992

Camion et al.

380/30 X

ART-UNIT: 222

PRIMARY-EXAMINER: Barron, Jr.; Gilberto

ATTY-AGENT-FIRM: Hicks; Richard J.

ABSTRACT:

A cryptographic method for communication and electronic signatures is described. The system includes at least one encoding device coupled to at least one decoding device by a communications channel. The method is a form of public-key or two-key cryptosystem, where the private decoding key is not feasibly determinable from the associated public encoding key. A block of ns bits of a message-to-be-transferred M (or key-to-be-distributed) is enciphered to ciphertext by first mapping M to a set $\{x_{sub.1}, x_{sub.2}, \dots, x_{sub.n}\}$, where $x_{sub.i} [0, 2^{sup.s})$. Then the ciphertext $\{y_{sub.1}, y_{sub.2}, \dots, y_{sub.m}\}$ is determined by $\text{##EQU1##} \bmod q_{sub.j}$, for $j=1$ to m' , and ##EQU2## for $j=m'+1$ to m , where ##EQU3## The encoding key (associated with the intended receiver) consists of integers $a_{sub.ij}$, $g_{sub.j}$, and positive fractions $f_{sub.i}$, for $i=1$ to n and for $j=1$ to m , and positive integers $q_{sub.j}$, for $j=1$ to m' . The ciphertext is deciphered (with a secret key known only to the intended receiver) by solving a knapsack ##EQU4## with secret superincreasing weights $\{b_{sub.1}, b_{sub.2}, \dots, b_{sub.n}\}$ and target value $b_{ident} \cdot \text{vertline.w}^{sup.-1} \cdot \text{vertline.w}'^{sup.-1} y_{\text{vertline..sub.Q}} \cdot \text{vertline..sub.P}$, where $y_{\text{ident}} \cdot \{y_{sub.1}, y_{sub.2}, \dots, y_{sub.m}\} \bmod \{q_{sub.1}, q_{sub.2}, \dots, q_{sub.m}\}$, ##EQU5## and w, w' , and $\{q_{sub.m'+1}, q_{sub.m'+2}, \dots, q_{sub.m}\}$ are secret integers. The resulting terms $\{x'_{sub.1}, x'_{sub.2}, \dots, x'_{sub.n}\}$ correspond to the original message terms $\{x_{sub.1}, x_{sub.2}, \dots, x_{sub.n}\}$.

20 Claims, 9 Drawing figures

[Previous Doc](#)[Next Doc](#)[Go to Doc#](#)